CLAIMS

What is claimed is:

1. A method of dynamically mitigating a noncompliant password, the method comprising the machine-implemented steps of:

obtaining a password from a user when the user attempts to access a service;

determining whether the password meets quality criteria; and

if the password does not meet the quality criteria, performing one or more responsive actions that relate to accessing the service.

2. The method of Claim 1, wherein the step of performing one or more responsive actions that relate to accessing the service comprises:

if the password meets the quality criteria, granting to the user a first level of access to the service, wherein the first level of access to the service is associated with the quality criteria;

if the password meets a second quality criteria, granting to the user a second level of access to the service, wherein the second level of access to the service is associated with the second quality criteria, wherein the second quality criteria is distinct from the quality criteria and wherein, if a particular password meets the quality criteria, then the password meets the second quality criteria.

3. The method of Claim 1, wherein the step of performing one or more responsive actions that relate to accessing the service comprises performing one or more of:

logging information related to the password;

sending a report about the password;

generating an alert about the password;

forcing a password change; or

blocking the user's access to the service.

4. The method of Claim 1, wherein the method further comprises, if the password does meet the quality criteria, providing user access to the service.

5. The method of Claim 1,, wherein the step of determining whether the password meets quality criteria further comprises one or more of the steps of:

performing a dictionary look-up based on the one or more symbols used in the password;

checking the length of the one or more symbols used in the password;

checking the number of unique characters of the one or more symbols used in the password;

checking the case of the characters in the one or more symbols used in the password;

checking the sequencing of characters in the one or more symbols used in the password; or

performing statistical analysis based on the one or more symbols used in the password.

6. The method of Claim 1, wherein the step of performing one or more responsive actions that relate to accessing the service comprises logging information related to the password.

7. The method of Claim 1, wherein the step of performing one or more responsive actions that relate to accessing the service comprises sending a report about the password.

8. The method of Claim 1, wherein the step of performing one or more responsive actions that relate to accessing the service comprises generating an alert about the password.

9. The method of Claim 1, wherein the step of performing one or more responsive actions that relate to accessing the service comprises forcing a password change.

10. The method of Claim 1, wherein the step of performing one or more responsive actions that relate to accessing the service comprises blocking the user's access to the service.

11. The method of Claim 1, wherein obtaining the password from the user comprises obtaining the password from the user via a graphical user interface.

12. The method of Claim 1, wherein obtaining the password from the user comprises obtaining the password from the user via an electronic interface.

13. The method of Claim 1, wherein the method further comprises the step of determining a quality score for the password, and wherein the step of determining whether the password meets quality criteria comprises comparing the quality score to a predefined threshold value.

14. The method of Claim 1, further comprising the steps of:

obtaining the password from a repository of passwords;

making a first determination whether the password meets quality criteria; and

storing in a particular machine-readable medium an indication of the first determination for the password;

wherein the step of determining whether the password meets quality criteria comprises accessing the particular machine-readable medium.

15. The method of Claim 1, wherein the user is associated with a particular user role, and wherein determining whether the password meets quality criteria comprises determining whether the password meets quality criteria for the particular user role.

16. The method of Claim 1, wherein determining whether the password meets quality criteria comprises determining whether the password meets quality criteria for the service.

17. The method of Claim 1, wherein the step of obtaining the password comprises an access service obtaining the password from the user when the user attempts to access the service, and wherein the access service comprises machine executable instructions executing on a particular machine, and the service comprises machine executable instruction executing on the same particular machine.

18. The method of Claim 1, wherein the step of obtaining the password comprises an access service obtaining the password from the user when the user attempts to access the service, and wherein the access service comprises machine executable instructions executing on a first machine and the service comprises machine executable instructions executing on a second machine, wherein the first machine is distinct from the second machine.

19. A method of dynamically mitigating a noncompliant password, the method comprising the machine-implemented steps of:

obtaining a password from a user when the user attempts to access a service;

determining whether the password meets quality criteria; and

if the password does not meet the quality criteria, performing one or more of:

forcing a password change; or

blocking the user's access to the service; and

wherein the step of determining whether the password meets quality criteria further comprises one or more of the steps of:

performing a dictionary look-up based on the one or more symbols used in the password;

checking the length of the one or more symbols used in the password;

checking the number of unique characters of the one or more symbols used in the password;

checking the case of the characters in the one or more symbols used in the password;

checking the sequencing of characters in the one or more symbols used in the password; or

performing statistical analysis based on the one or more symbols used in the password.

20. A machine-readable medium carrying one or more sequences of instructions for dynamically mitigating a noncompliant password, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of:

obtaining a password from a user when the user attempts to access a service;

determining whether the password meets quality criteria; and

if the password does not meet the quality criteria, performing one or more responsive actions that relate to accessing the service.

21. The machine-readable medium of Claim 20, wherein the step of performing one or more responsive actions that relate to accessing the service comprises:

if the password meets the quality criteria, granting to the user a first level of access to the service, wherein the first level of access to the service is associated with the quality criteria;

if the password meets a second quality criteria, granting to the user a second level of access to the service, wherein the second level of access to the service is associated with the second quality criteria, wherein the second quality criteria is distinct from the quality criteria and wherein, if a particular password meets the quality criteria, then the password meets the second quality criteria.

22. The machine-readable medium of Claim 20, wherein the step of performing one or more responsive actions that relate to accessing the service comprises performing one or more of:

logging information related to the password;

sending a report about the password;

generating an alert about the password;

forcing a password change; or

blocking the user's access to the service.

23. The machine-readable medium of Claim 20, further comprising instructions which, when executed by the one or more processors, cause the one or more processors to carry out the step of, if the password does meet the quality criteria, providing user access to the service.

24. The machine-readable medium of Claim 20, wherein the step of determining whether the password meets quality criteria further comprises one or more of the steps of:

performing a dictionary look-up based on the one or more symbols used in the password;

checking the length of the one or more symbols used in the password;

checking the number of unique characters of the one or more symbols used in the password;

checking the case of the characters in the one or more symbols used in the password;

checking the sequencing of characters in the one or more symbols used in the password; or

performing statistical analysis based on the one or more symbols used in the password.

25. The machine-readable medium of Claim 20, wherein the step of performing one or more responsive actions that relate to accessing the service comprises logging information related to the password.

26. The machine-readable medium of Claim 20, wherein the step of performing one or more responsive actions that relate to accessing the service comprises sending a report about the password.

27. The machine-readable medium of Claim 20, wherein the step of performing one or more responsive actions that relate to accessing the service comprises generating an alert about the password.

28. The machine-readable medium of Claim 20, wherein the step of performing one or more responsive actions that relate to accessing the service comprises forcing a password change.

29. The machine-readable medium of Claim 20, wherein the step of performing one or more responsive actions that relate to accessing the service comprises blocking the user's access to the service.

30. The machine-readable medium of Claim 20, wherein obtaining the password from the user comprises obtaining the password from the user via a graphical user interface.

31. The machine-readable medium of Claim 20, wherein obtaining the password from the user comprises obtaining the password from the user via an electronic interface.

32. The machine-readable medium of Claim 20, further comprising instructions which, when executed by the one or more processors, cause the one or more processors to carry out the step of determining a quality score for the password, and wherein the step of determining whether the password meets quality criteria comprises comparing the quality score to a predefined threshold value.

33. The machine-readable medium of Claim 20, further comprising instructions which, when executed by the one or more processors, cause the one or more processors to carry out the steps of:

obtaining the password from a repository of passwords;

making a first determination whether the password meets quality criteria; and

storing in a particular machine-readable medium an indication of the first determination for the password;

and wherein the step of determining whether the password meets quality criteria comprises accessing the particular machine-readable medium.

34. The machine-readable medium of Claim 20, wherein the user is associated with a particular user role, and wherein determining whether the password meets quality criteria comprises determining whether the password meets quality criteria for the particular user role.

35. The machine-readable medium of Claim 20, wherein determining whether the password meets quality criteria comprises determining whether the password meets quality criteria for the service.

36. An apparatus for dynamically mitigating a noncompliant password, comprising:
means for obtaining a password from a user when the user attempts to access a service;
means for determining whether the password meets quality criteria; and
means for performing one or more responsive actions that relate to accessing the service if the password does not meet the quality criteria.

37. The apparatus of Claim 36, wherein the means for performing one or more responsive actions that relate to accessing the service comprises:
means for granting to the user a first level of access to the service, if the password meets the quality criteria, wherein the first level of access to the service is associated with the quality criteria;
means for granting to the user a second level of access to the service, if the password meets a second quality criteria, wherein the second level of access to the service is associated with the second quality criteria, wherein the second quality criteria is distinct from the quality criteria and wherein, if a particular password meets the quality criteria, then the password meets the second quality criteria..

38. The apparatus of Claim 36, wherein the means for performing one or more responsive actions that relate to accessing the service comprises one or more of:

means for logging information related to the password;

means for sending a report about the password;

means for generating an alert about the password;

means for forcing a password change; or

means for blocking the user's access to the service.

39. The apparatus of Claim 36, wherein the apparatus further comprises means for providing user access to the service if the password does meet the quality criteria.

40. The apparatus of Claim 36, wherein the means for determining whether the password meets quality criteria further comprises one or more of:

means for performing a dictionary look-up based on the one or more symbols used in the password;

means for checking the length of the one or more symbols used in the password;

means for checking the number of unique characters of the one or more symbols used in the password;

means for checking the case of the characters in the one or more symbols used in the password;

means for checking the sequencing of characters in the one or more symbols used in the password; or

means for performing statistical analysis based on the one or more symbols used in the password.

41. The apparatus of Claim 36, wherein the means for performing one or more responsive actions that relate to accessing the service comprises means for logging information related to the password.

42. The apparatus of Claim 36, wherein the means for performing one or more responsive actions that relate to accessing the service comprises means for sending a report about the password.

43. The apparatus of Claim 36, wherein the means for performing one or more responsive actions that relate to accessing the service comprises means for generating an alert about the password.

44. The apparatus of Claim 36, wherein the means for performing one or more responsive actions that relate to accessing the service comprises means for forcing a password change.

45. The apparatus of Claim 36, wherein the means for performing one or more responsive actions that relate to accessing the service comprises means for blocking the user's access to the service.

46. The apparatus of Claim 36, wherein the means for obtaining the password from the user comprises means for obtaining the password from the user via a graphical user interface.

47. The apparatus of Claim 36, wherein the means for obtaining the password from the user comprises means for obtaining the password from the user via an electronic interface.

48. The apparatus of Claim 36, wherein the apparatus further comprises means for determining a quality score for the password, and wherein the means for determining whether the password meets quality criteria comprises means for comparing the quality score to a predefined threshold value.

49. The apparatus of Claim 36, further comprising:

means for obtaining the password from a repository of passwords;

means for making a first determination whether the password meets quality criteria; and

means for storing in a particular machine-readable medium an indication of the first determination for the password;

and wherein the means for determining whether the password meets quality criteria comprises means for accessing the particular machine-readable medium.

50. The apparatus of Claim 36, wherein the user is associated with a particular user role, and wherein means for determining whether the password meets quality criteria comprises means for determining whether the password meets quality criteria for the particular user role.

51. The apparatus of Claim 36, wherein means for determining whether the password meets quality criteria comprises means for determining whether the password meets quality criteria for the service.

52. The apparatus of Claim 36, wherein the means for obtaining the password comprises means for an access service to obtain the password from the user when the user attempts to access the service, and wherein the access service comprises means for executing on a particular machine, and wherein the service comprises means for executing on the same particular machine.

53. The apparatus of Claim 36, wherein the means for obtaining the password comprises means for an access service to obtain the password from the user when the user attempts to access the service, and wherein the access service comprises means for executing on a first machine and the service comprises means for executing on a second machine, wherein the first machine is distinct from the second machine.

54. An apparatus for dynamically mitigating a noncompliant password, comprising:
a network interface that is coupled to the data network for receiving one or more packet flows therefrom;
a processor;
one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:
obtaining a password from a user when the user attempts to access a service;
determining whether the password meets quality criteria; and
if the password does not meet the quality criteria, performing one or more responsive actions that relate to accessing the service.

55. The apparatus of Claim 54, wherein the step of performing one or more responsive actions that relate to accessing the service comprises:
if the password meets the quality criteria, granting to the user a first level of access to the service, wherein the first level of access to the service is associated with the quality criteria;
if the password meets a second quality criteria, granting to the user a second level of access to the service, wherein the second level of access to the service is associated with the second quality criteria, wherein the second quality criteria is distinct from the quality criteria and wherein, if a particular password meets the quality criteria, then the password meets the second quality criteria.

56. The apparatus of Claim 54, wherein the step of performing one or more responsive actions that relate to accessing the service comprises performing one or more of:
logging information related to the password;
sending a report about the password;
generating an alert about the password;
forcing a password change; or
blocking the user's access to the service.

57. The apparatus of Claim 54, wherein the apparatus further comprises one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the step of, if the password does meet the quality criteria, providing user access to the service.

58. The apparatus of Claim 54, wherein the step of determining whether the password meets quality criteria comprises one or more of the steps of:

performing a dictionary look-up based on the one or more symbols used in the password;

checking the length of the one or more symbols used in the password;

checking the number of unique characters of the one or more symbols used in the password;

checking the case of the characters in the one or more symbols used in the password;

checking the sequencing of characters in the one or more symbols used in the password; or

performing statistical analysis based on the one or more symbols used in the password.

59. The apparatus of Claim 54, wherein the step of performing one or more responsive actions that relate to accessing the service comprises logging information related to the password.

60. The apparatus of Claim 54, wherein the step of performing one or more responsive actions that relate to accessing the service comprises sending a report about the password.

61. The apparatus of Claim 54, wherein the step of performing one or more responsive actions that relate to accessing the service comprises generating an alert about the password.

62. The apparatus of Claim 54, wherein the step of performing one or more responsive actions that relate to accessing the service comprises forcing a password change.

63. The apparatus of Claim 54, wherein the step of performing one or more responsive actions that relate to accessing the service comprises blocking the user's access to the service.

64. The apparatus of Claim 54, wherein obtaining the password from the user comprises obtaining the password from the user via a graphical user interface.

65. The apparatus of Claim 54, wherein obtaining the password from the user comprises obtaining the password from the user via an electronic interface.

66. The apparatus of Claim 54, wherein the apparatus further comprises one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the step of determining a quality score for the password, and wherein the step of determining whether the password meets quality criteria comprises comparing the quality score to a predefined threshold value.

67. The apparatus of Claim 54, further comprising one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:

obtaining the password from a repository of passwords;

making a first determination whether the password meets quality criteria; and

storing in a particular machine-readable medium an indication of the first determination for the password;

and wherein the step of determining whether the password meets quality criteria comprises accessing the particular machine-readable medium.

68. The apparatus of Claim 54, wherein the user is associated with a particular user role, and wherein determining whether the password meets quality criteria comprises determining whether the password meets quality criteria for the particular user role.

69. The apparatus of Claim 54, wherein determining whether the password meets quality criteria comprises determining whether the password meets quality criteria for the service.

70. The apparatus of Claim 54, wherein the step of obtaining the password comprises an access service obtaining the password from the user when the user attempts to access the service, and wherein the access service comprises machine executable instructions executing on the apparatus, and the service comprises machine executable instruction executing on the same apparatus.

71. The apparatus of Claim 54, wherein the step of obtaining the password comprises an access service obtaining the password from the user when the user attempts to access the service, and wherein the access service comprises machine executable instructions executing on a first machine and the service comprises machine executable instructions executing on a second machine, wherein the first machine is distinct from the second machine.